

GENERALIZED INVARIANTS OF REFLECTION GROUPS IN RANK TWO

JAUME AGUADÉ

ABSTRACT. For each subgroup of $GL_2(\mathbb{F}_p)$ or order divisible by p , generated by (pseudo-)reflections, we compute the ideals of stable and generalized invariants. These groups and these ideals are related to the cohomology of compact Lie groups, Kac-Moody groups and p -compact groups.

1. INTRODUCTION

The invariant theory of finite reflection groups (also called pseudoreflection groups) in positive characteristic dividing the order of the group displays a series of phenomena which do not appear when the order of the group is a unit in the base field. Some of these phenomena are not yet well understood. Generalized invariants and stable invariants are two of these phenomena. They were defined by Kac in 1985 ([11]) based on work of Demazure in 1973 ([9]), to provide a purely Weyl group explanation of the mod p cohomology of the compact connected Lie groups. If the order of the reflection group W is prime to p , then both generalized and stable invariants coincide with the standard polynomial invariants of W , but if this non-modularity condition fails, the generalized invariants and the stable invariants seem to be very hard to compute and they are only known in a few trivial cases. For instance, neither the generalized nor the stable invariants of the general linear group over a finite field are known and it has been conjectured that they are trivial, in the sense that they coincide with the ordinary invariants, i.e. the Dickson invariants.

In this paper we compute the generalized and the stable invariants of all reflection subgroups of $GL_2(\mathbb{F}_p)$ of order divisible by p . Our results support the conjecture above. In a final section, we review the appearance of these rank two reflection groups in topology, as mod p reductions of Weyl groups of some families of topological groups, like Lie groups, Kac-Moody groups or p -compact groups.

2. PRELIMINARIES AND NOTATIONS

Most of what we need in this paper can be found in the introduction to [16], but we include it here for completeness and in order to fix the notations that we will be using along the paper. The twin books [19] and [6] are excellent references for anything that is stated here without a proof.

An element $\sigma \in GL_n(\mathbb{F}_p)$ is a *reflection* if $\sigma - 1$ has rank 1. Some authors call this a *pseudoreflection* and reserve the word reflection for the case in which σ is diagonalizable and $\sigma^2 = 1$. We call x_1, \dots, x_n the standard basis of the \mathbb{F}_p -vector

Key words and phrases. Reflection group, polynomial invariants, generalized invariants, stable invariants.

The author is partially supported by grants MTM2013-42293-P and 2009SGR-1092.

space \mathbb{F}_p^n and then we consider the linear action of $GL_n(\mathbb{F}_p)$ on the polynomial ring $P_n := \mathbb{F}_p[x_1, \dots, x_n]$. Some authors consider the dual action. If G is any subgroup of $GL_n(\mathbb{F}_p)$, then the polynomials in P_n invariant under all $g \in G$ form the ring of invariants P_n^G . If this ring of invariants is a polynomial ring, then the group G is generated by reflections and P_n is a free P_n^G -module of rank equal to $|G|$. If a group $G \subseteq GL_n(\mathbb{F}_p)$ is generated by reflections we say that G is a *reflection group*, but we have to keep in mind that being a reflection group is not an intrinsic property of a group, but a property of a representation of this group.

The ring of coinvariants of $G \subseteq GL_n(\mathbb{F}_p)$ is the quotient of P_n by the ideal $J_1(G)$ generated by the elements in P_n^G of positive degree.

$$(P_n)_G := P_n/J_1(G) = \mathbb{F}_p \otimes_{P_n^G} P_n.$$

If P_n^G is a polynomial algebra, then $(P_n)_G$ is an algebra with Poincaré duality. The ring of coinvariants inherits an action of G and if $|G|$ is prime to p , then $(P_n)_G$ coincides with the regular representation of G . In particular, $(P_n)_G$ has no invariants of positive degree. However, when p divides the order of G , the ring $(P_n)_G$ can have invariants of positive degree and we can inductively define a chain of ideals of P_n

$$J_1(G) \subseteq J_2(G) \subseteq \dots$$

as follows:

$$A_0 := P_n, \quad A_i := (A_{i-1})_G, \quad J_i(G) := \text{Ker}\{P_n \rightarrow A_i\}.$$

We can also consider the ideal $J_\infty(G) := \cup_i J_i(G)$ which is called the ideal of *stable invariants* of G . As we said before, if the order of G is prime to p , all these ideals coincide with the ideal $J_1(G)$ of ordinary invariants of G . We also refer to the sequence $\{J_i(G)\}_{i=1}^\infty$ as the sequence of ideals of stable invariants of G .

The ring of invariants of a reflection group of order prime to p is a polynomial algebra, but this fails if we do not assume that $|G|$ is prime to p . Hence, one can ask about which reflection groups in $GL_n(\mathbb{F}_p)$ have polynomial rings of invariants. The work of Kemper-Malle ([14]) provides a complete list of all irreducible groups in $GL_n(\mathbb{F}_{p^r})$ with polynomial rings of invariants, for all values of n, p, r .

Given a reflection $\sigma \in GL_n(\mathbb{F}_p)$, Demazure ([9]) and Kac-Peterson ([12], [11]) defined an \mathbb{F}_p -linear operator $\Delta_\sigma : P_n \rightarrow P_n$ of degree -1 as follows. Chose a non zero vector v_σ in the image of $\sigma - 1$, then

$$\Delta_\sigma(f) := \frac{\sigma(f) - f}{v_\sigma}.$$

These operators are well defined up to a non zero multiplicative constant. They behave as twisted derivations

$$\Delta_\sigma(fg) = \Delta_\sigma(f)g + \sigma(f)\Delta_\sigma(g)$$

and play an important role in understanding the cohomology of classifying spaces of compact connected Lie groups (and, more in general, Kac-Moody groups) at torsion primes (see [11] and [17]). These operators were used by Kac-Peterson to define the *ideal of generalized invariants* $I(\mathcal{S})$ of a set of reflections $\mathcal{S} \subseteq GL_n(\mathbb{F}_p)$. We say that a polynomial $f \in P_n$ of positive degree k is a generalized invariant with respect to \mathcal{S} if for any sequence $\{\sigma_1, \dots, \sigma_k\}$ of elements of \mathcal{S} we have that

$$\Delta_{\sigma_1} \cdots \Delta_{\sigma_k}(f) = 0.$$

It can be proved ([16], lemma 2.1) that the generalized invariants form an ideal $I(\mathcal{S}) \subset P_n$. By definition, this ideal depends on the set \mathcal{S} and not just on the reflection group $G(\mathcal{S})$ generated by \mathcal{S} . There is an interesting relation between generalized invariants and stable invariants ([16], lemma 3.2)

$$J_1(G(\mathcal{S})) \subseteq I(\mathcal{S}) \subseteq J_\infty(G(\mathcal{S})).$$

In general, these three ideals can be different. If the reflections in \mathcal{S} are diagonalizable, then $I(\mathcal{S}) = J_\infty(G(\mathcal{S}))$. If the order of $G(\mathcal{S})$ is prime to p , then ordinary, stable and generalized invariants coincide.

As said before, for reflection groups of order divisible by p the ring of invariants may fail to be a polynomial ring. However, a very interesting property of the ideal of generalized invariants is given in the following theorem of Kac-Peterson ([12]): $I(\mathcal{S})$ is always generated by a regular sequence of length n .

In this paper we will be dealing with the case of $GL_2(\mathbb{F}_p)$ and we use the following notations. P will be the polynomial ring on two generators $P := \mathbb{F}_p[x, y]$. ζ will denote a generator of \mathbb{F}_p^* . We denote $\omega, \omega' \in GL_2(\mathbb{F}_p)$ the reflections

$$\omega := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \omega' := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

The operators associated to these two reflections (choosing $v_\omega = (0, 1)$ and $v_{\omega'} = (1, 0)$) are denoted Δ and $\overline{\Delta}$, respectively. Diagonal matrices will be denoted this way

$$D(a, b) := \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}.$$

There are some polynomials in P that will appear often and we fix here the notation that we use for them.

$$\begin{aligned} \delta &:= xy^p - x^p y \\ d_1 &:= \frac{1}{\delta} (xy^{p^2} - x^{p^2} y) \\ d_0 &:= \frac{1}{\delta} (x^p y^{p^2} - x^{p^2} y^p) \\ \gamma_i &:= x^{i(p-1)} - x^{p-1} y^{(i-1)(p-1)} + y^{i(p-1)}, \quad i \geq 1. \end{aligned}$$

d_0, d_1 are the well known Dickson polynomials and the polynomials γ_i will appear in the computation of the stable invariants of the group $SL_2(\mathbb{F}_p)$.

Since we are only considering homogeneous polynomials, we sometimes simplify the notation by substituting the exponents of one of the variables by an asterisk. For instance, we can write $\gamma_i = x^{i(p-1)} - x^{p-1} y^* + y^*$.

3. REFLECTION GROUPS IN DIMENSION TWO AND THEIR INVARIANTS

The well known classification of subgroups of $GL_2(k)$ for a finite field k (see [21], 3.6) makes it easy to determine all reflection subgroups of $GL_2(\mathbb{F}_p)$. Let us introduce the following subgroups of $GL_2(\mathbb{F}_p)$.

- For each $r|p-1$ let L^r be the subgroup of all matrices $A \in GL_2(\mathbb{F}_p)$ such that A^r has determinant 1. If $r = 1$, this is the special linear group $SL_2(\mathbb{F}_p)$; if $r = p-1$, this is the full linear group $GL_2(\mathbb{F}_p)$. L^r is a reflection group of order $rp(p^2 - 1)$ generated by the reflections $\omega, \omega', D(\zeta^{\frac{p-1}{r}}, 1)$.

- For each $r, s|p-1$ let $U_{r,s}$ be the subgroup of all upper triangular matrices

$$\begin{pmatrix} \alpha & \lambda \\ 0 & \beta \end{pmatrix} \in GL_2(\mathbb{F}_p)$$

such that $\alpha^r = \beta^s = 1$. It is a reducible reflection group of order rsp generated by the reflections ω , $D(\zeta^{\frac{p-1}{r}}, 1)$, $D(1, \zeta^{\frac{p-1}{s}})$. $U_{1,1}$ is the cyclic group of order p in its representation as a Sylow subgroup of $GL_2(\mathbb{F}_p)$. As abstract groups, both $U_{2,1}$ and $U_{1,2}$ are isomorphic to the dihedral group of order $2p$, but they are not conjugate. These groups are considered in [19] (pages 128–129), [16] and also in [3] and [2] where they appeared as mod p reductions of the (infinite) Weyl groups of some Kac-Moody groups.

Theorem 3.1. *Let $G \subseteq GL_2(\mathbb{F}_p)$ be a reflection group with $|G| \equiv 0(p)$. Up to conjugation,*

- (1) $G = U_{r,s}$ for some $r, s|p-1$, or
- (2) $G = L^r$ for some $r|p-1$.

Proof. The result is straightforward for $p = 2$ so we can assume $p > 2$. According to Theorem 8.1 in [14], the table 8.2 in [14] lists all irreducible primitive reflection groups in dimension two. The first entry in the list consists of groups G in characteristic p such that $SL_2(\mathbb{F}_p) \triangleleft G$. These are the groups L^r . The second entry consists of groups G in characteristic 3 such that $SL_2(\mathbb{F}_3) \triangleleft G$. Since $|SL_2(\mathbb{F}_3)| = 120$, none of these groups can be a subgroup of $GL_2(\mathbb{F}_3)$. All other groups in the list are representations over finite fields of the finite unitary reflection groups of dimension two in the list of Shephard-Todd ([18]). All these groups have order prime to p . Hence, we only need to check the imprimitive groups and the reducible groups.

Let θ_m denote a primitive m -th root of unity. The imprimitive reflection groups are the groups

$$G(m, r) := \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \theta_m^i & 0 \\ 0 & \theta_m^j \end{pmatrix}, i + j \equiv 0(r) \right\rangle$$

for any m and any $r|m$. This group has order $2m^2/r$. The orthogonal groups $O_2^+(\mathbb{F}_p)$ and $O_2^-(\mathbb{F}_p)$ are particular cases of these groups. Notice that $D(\theta_m, \theta_m^{-1}) \in G(m, r)$ hence, if the group $G(m, r)$ can be represented in $GL_2(\mathbb{F}_p)$ then $\theta_m + \theta_m^{-1} \in \mathbb{F}_p$. Since $\mathbb{F}_p(\theta_m)$ is an extension of $\mathbb{F}_p(\theta_m + \theta_m^{-1})$ of degree ≤ 2 , if $G(m, r)$ can be represented in $GL_2(\mathbb{F}_p)$, then $\theta_m \in \mathbb{F}_{p^2}$ and $m|p^2 - 1$. This shows that all imprimitive reflection groups in $GL_2(\mathbb{F}_p)$ have order prime to p .

Let G be a reducible reflection subgroup of $GL_2(\mathbb{F}_p)$ and assume that G is a subgroup of the group of upper triangular matrices in $GL_2(\mathbb{F}_p)$.

If $\begin{pmatrix} \alpha & \lambda \\ 0 & \beta \end{pmatrix}$ is a reflection, then $\alpha = 1$ or $\beta = 1$. Since p divides the order of G , all upper unitriangular matrices are in G . Observe that

$$\begin{aligned} \begin{pmatrix} 1 & -\lambda/\beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & \beta \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix} \\ \begin{pmatrix} 1 & -\mu \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & \mu \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Hence, if G is generated by reflections

$$G = \left\langle \begin{pmatrix} 1 & \lambda_i \\ 0 & \beta_i \end{pmatrix}, \begin{pmatrix} \alpha_j & \mu_j \\ 0 & 1 \end{pmatrix}, i = 1, \dots, n, j = 1, \dots, m \right\rangle$$

then $D(\alpha_i, 1)$, $D(1, \beta_j)$, $\omega' \in G$, $i = 1, \dots, n$, $j = 1, \dots, m$. Let r be the order of the subgroup of \mathbb{F}_p^* generated by $\alpha_1, \dots, \alpha_n$ and let s be the subgroup of \mathbb{F}_p^* generated by β_1, \dots, β_m . Then, it is clear that $G = U_{r,s}$. \square

The ring of invariants of the general linear group is the well known Dickson Algebra ([6], [19]). In the case of dimension two,

$$P^{GL_2(\mathbb{F}_p)} = \mathbb{F}_p[d_1, d_0], \quad |d_1| = p^2 - p, |d_0| = p^2 - 1.$$

Notice that $d_0 = \delta^{p-1}$. The invariants of the groups L^r for $r|p-1$ are also well known:

$$P^{L^r} = \mathbb{F}_p[d_1, \delta^r].$$

The invariants of the reducible reflection groups $U_{r,s}$ are as follows.

Proposition 3.2. *The invariants of $U_{r,s}$ form a polynomial algebra with generators x^r and $(y^p - x^{p-1}y)^s$.*

Proof. It is trivial to check that x^r and $(y^p - x^{p-1}y)^s$ are invariant under the generators of $U_{r,s}$. Since the Jacobian of these two polynomials does not vanish, we can use proposition 16 in [13] to conclude that

$$P^{U_{r,s}} = \mathbb{F}_p[x^r, (y^p - x^{p-1}y)^s].$$

\square

4. BASES FOR RINGS OF COINVARIANTS

In this section we obtain explicit bases of P over P^G for each reflection group $G \subseteq GL_2(\mathbb{F}_p)$. We first state some useful identities involving the polynomials d_1, d_0, δ , which will play an important role in the computations in this paper. The proofs are easy, either by a direct computation or using induction, and we omit the details.

Proposition 4.1. *Assume $p > 2$. Then*

- (1) $d_1 = \sum_{i=0}^p x^{(p-1)i} y^{(p-1)(p-i)}$.
- (2) $y^{p^2-1} = y^{p-1}d_1 - d_0$.
- (3) $y^{p^2-p+r} = y^r d_1 - x^{p-r-1}(y^{p-1} - x^{p-1})^{p-r-1} \delta^r$ for any $0 \leq r \leq p-1$.
- (4) $d_1 = x^{p^2-p} + y^{p^2-p} - x^{p-1}y^* - \delta \sum_{k=1}^{p-2} k x^* y^{k(p-1)-1}$.
- (5) Let $i \geq p$, $j \geq 1$ and let $a, b > 0$ be integers such that $i = a(p-1) + b$ and $0 < b \leq p-1$. Then

$$x^i y^j = x^b y^* + \langle \delta \rangle.$$

- (6) Let $0 < r < p-1$ and $j \geq r$. Then any monomial $x^i y^j$ can be written as an \mathbb{F}_p -linear combination

$$x^i y^j = \sum_{s=0}^{rp-1} \lambda_s x^s y^* + \langle \delta^r \rangle.$$

\square

Let $r|p-1$. Define

$$\Omega^r := \left\{ x^i y^j \left| \begin{array}{l} 0 \leq i \leq rp-1 \\ 0 \leq j \leq p^2-p+r-1 \end{array} \right. \right\} \cup \left\{ x^i y^j \left| \begin{array}{l} rp \leq i \leq p^2-p-1 \\ 0 \leq j \leq r-1 \end{array} \right. \right\}.$$

Notice that $|\Omega^r| = rp(p^2 - 1) = |L^r|$. As suggested by the definition above, it is useful to imagine Ω^r as consisting of two blocks: a first block which contains all monomials which divide $x^{rp-1}y^{p^2-p+r-1}$ and a second block with all monomials $x^i y^j$ for $rp \leq i \leq p^2 - p - 1$, $0 \leq j \leq r - 1$. This second block only appears if $r < p - 1$.

Proposition 4.2. Ω^r is a P^{L^r} -basis for P .

Proof. It is enough to prove that the monomials in Ω^r generate P as a P^{L^r} -module. We prove this by induction on the degree. Let f be a polynomial of degree n and write $n = a(p^2 - p) + b$ with $a, b \geq 0$ and $0 \leq b < p^2 - p$. Then it is clear that we can write $f = \lambda d_1^a x^b + yf'$ for some $\lambda \in \mathbb{F}_p$, $f' \in P$. By induction, we can write $f' = \sum h_i \alpha_i$ for some $h_i \in P^{L^r}$, $\alpha_i \in \Omega^r$. It is clear that for any $\alpha \in \Omega^r$ we have $y\alpha \in \Omega^r$, except in the following two cases:

- (1) $\alpha = x^i y^{p^2-p+r-1}$, $0 \leq i \leq rp - 1$.
In this case, formula (3) in 4.1 tells us that $y\alpha = x^i y^{p^2-p+r} = d_1 x^i y^r - \delta^r h$ for some $h \in P$. By induction, h is in $P^{L^r} \langle \Omega^r \rangle$ and so is $y\alpha$.
- (2) $\alpha = x^i y^{r-1}$, $r < p - 1$, $rp \leq i \leq p^2 - p - 1$.
In this case, we use 4.1(6) to write the monomial $x^i y^r$ as

$$x^i y^r = \sum_{s=0}^{rp-1} \lambda_s x^s y^* + \delta^r h.$$

Then, we can apply induction on h to finish the proof. □

The case $r = p - 1$ of this result was known since the work of Campbell et al. ([8]) who computed a basis for the coinvariants of the group $GL_n(\mathbb{F}_p)$ for any n .

The case of the reducible groups $U_{r,s}$ is similar but easier.

Proposition 4.3. For any $r, s | p - 1$ the monomials

$$\Gamma_{r,s} := \{x^i y^j \mid 0 \leq i \leq r - 1, 0 \leq j \leq ps - 1\}$$

form a basis of P over $P^{U_{r,s}}$.

Proof. Again, it is enough to show that these monomials generate P over $P^{U_{r,s}}$. Recall from 3.2 that the ring of invariants of $U_{r,s}$ is generated by x^r and $\rho = (y^p - x^{p-1}y)^s$. If f is any polynomial, we can write $f = \lambda \rho^a y^b + xh$ for some $a \geq 0$, $0 \leq b < ps$, $h \in P$. By induction on the degree, the polynomial h is in the span of $\Gamma_{r,s}$. Then, for any $\alpha \in \Gamma_{r,s}$ we have $x\alpha \in \Gamma_{r,s}$, except for the case of $\alpha = x^{r-1}y^j$ for $0 \leq j < ps$, but in this case $x\alpha = x^r y^j \in P^{U_{r,s}} \langle \Gamma_{r,s} \rangle$. □

In all these cases, the ring of coinvariants is a Poincaré duality algebra. The fundamental class μ is $x^{rp-1}y^{p^2-p+r-1}$ for the group L^r and $x^{r-1}y^{ps-1}$ for the group $U_{r,s}$.

5. IDEALS OF STABLE INVARIANTS

In this section we compute the sequence of ideals of stable invariants of the reflection groups in $GL_2(\mathbb{F}_p)$. We start with the harder case of the groups L^r . First, we need to compute the invariants of L^r acting on the coinvariant algebra P_{L^r} . The following lemma on binomial coefficients modulo p will be used in the proofs in this section.

Lemma 5.1. *Let $0 \leq i < p$, $1 \leq k < p$. Then*

$$\sum_{t=0}^{k-1} \binom{k(p-1)}{i+t(p-1)} \equiv (-1)^i \pmod{p}.$$

Proof. We need a well known fact on the computation of binomial coefficients modulo a prime (see [20], lemma 2.6). If $a = \sum a_i p^i$, $b = \sum b_i p^i$ are the base p series for the integers a and b , then

$$\binom{a}{b} \equiv \prod \binom{a_i}{b_i} \pmod{p}.$$

Using this fact we can proceed as follows. If $i < k$ then

$$\begin{aligned} \sum_{t=0}^{k-1} \binom{k(p-1)}{i+t(p-1)} &= \sum_{t=0}^i \binom{k(p-1)}{i+t(p-1)} + \sum_{t=i+1}^{k-1} \binom{k(p-1)}{i+t(p-1)} \\ &\equiv \sum_{t=0}^i \binom{k-1}{t} \binom{p-k}{i-t} + \sum_{t=i+1}^{k-1} \binom{k-1}{t-1} \binom{p-k}{p+i-t}. \end{aligned}$$

The first term is equal to $\binom{p-1}{i} \equiv (-1)^i (p)$ and the second term vanishes because $p+i-t > p-k$. Notice that the same argument holds for $i \geq k$. \square

Theorem 5.2. *Let A be the elements of positive degree in the coinvariant algebra P_{L^r} and let A^{L^r} denote the \mathbb{F}_p -vector space of L^r -invariant elements of A . Then*

- (1) *If $r > 1$, then $A^{L^r} = 0$.*
- (2) *If $r = 1$, then A^{L^r} is generated by the following elements:*
 - (a) *The fundamental class $\mu = x^{p-1}y^{p^2-p}$.*
 - (b) *The elements γ_i for $i = 2, \dots, p-1$.*

Proof. The case of $p = 2$ can be easily worked out directly (see example 1.10 in [16]), so we assume that $p > 2$. In proposition 4.2 we have found an \mathbb{F}_p -basis Ω^r for P_{L^r} so an element in P_{L^r} of degree n can be uniquely written as

$$f = \sum_{\substack{i+j=n \\ x^i y^j \in \Omega^r}} \lambda_{ij} x^i y^j.$$

The matrices $D(\zeta^{\frac{p-1}{r}}, 1)$, $D(1, \zeta^{\frac{p-1}{r}})$, $D(\zeta, \zeta^{-1}) \in L^r$ act diagonally on the elements of the basis Ω^r . Hence, if f is invariant then the coefficients λ_{ij} must vanish except when $i, j \equiv 0 (r)$ and $2i \equiv n (p-1)$. Lets call this “sparseness”.

Recall that we are considering the basis Ω^r as formed by two blocks. Then, we can distinguish two cases for an hypothetical invariant f , depending if f contains monomials from both of the blocks (this is only possible if $r < p-1$) or it only contains monomials from the first block. Let us consider first the case in which there is no monomial from the second block of Ω^r . Then,

$$f = \sum_{i=k_0}^{rp-1} \lambda_i x^i y^{n-i}$$

where $k_0 = \max\{0, n - p^2 + p - r + 1\}$. In the extreme case $k_0 = rp - 1$, f is a multiple of the fundamental class $\mu = x^{rp-1}y^{p^2-p+r-1}$ which can only be an invariant if $r = 1$. In this case, this fundamentals class μ of the Poincaré duality

algebra of coinvariants of L^1 is indeed invariant under the action of L^1 because any element $g \in L^1$ must transform the fundamental class μ into some multiple of itself $\chi(g)\mu$, where χ is a character of L^1 . But $L^1 = SL_2(\mathbb{F}_p)$ has no non trivial characters.

Assume $k_0 < rp-1$. Using 4.1(3) we see that $y^k = 0$ in A whenever $k \geq p^2 - p + r$. If we assume that f is invariant under ω , we get

$$f = \omega f = \sum_{i=k_0}^{rp-1} \sum_{j=0}^i \binom{i}{j} \lambda_i x^j y^{n-j} \equiv \sum_{i=k_0}^{rp-1} \sum_{j=k_0}^i \binom{i}{j} \lambda_i x^j y^{n-j} = \sum_{j=k_0}^{rp-1} \left(\sum_{i=j}^{rp-1} \binom{i}{j} \lambda_i \right) x^j y^{n-j}.$$

Since all monomials here belong to the basis Ω^r , their coefficients must agree with the coefficients in f and we get a system of linear equations for the coefficients λ_i :

$$\sum_{j=i+1}^{rp-1} \binom{j}{i} \lambda_j = 0, \quad i = k_0, \dots, rp-2.$$

The last equation gives $\lambda_{rp-1} = 0$ and we can prove recursively that $\lambda_i = 0$ for $i > 0$ by noticing that $i \equiv 0 \pmod{p}$ and $\lambda_i \neq 0$ imply $i \equiv 0 \pmod{pr}$ which is not possible.

Hence, f must be a multiple of y^n . If y^n were invariant under $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ then

$$y^n - x^n \in \langle d_1, \delta^r \rangle \subset \langle d_1, \delta \rangle.$$

If $n < p^2 - p = |d_1|$, then this is not possible because δ is divisible by x . Assume $n \geq p^2 - p$. This implies $n = p^2 - p$. Using 4.1(4) we deduce

$$2y^{p^2-p} - x^{p-1}y^{p^2-2p+1} \in \langle d_1, \delta \rangle$$

which is not possible since these two monomials are in Ω^1 which is a basis of P over $P^{L^1} = \mathbb{F}_p[d_1, \delta]$.

The conclusion so far is that the only invariants in A which do not involve monomials from the second block of Ω^r are the scalar multiples of $\mu = x^{p-1}y^{p^2-p}$ for $r = 1$. Let us investigate now under which conditions a polynomial involving monomials from the second block of Ω^r can be L^r -invariant. By sparseness, the only monomial from the second block that can appear is x^n for $n \equiv 0 \pmod{p-1}$. Assume that $f = \sum_{i=0}^{rp-1} \lambda_i x^i y^{n-i} + x^n$ is L^r -invariant with $rp \leq n \leq p^2 - p - 1$. We must have $r < p-1$ and $n \equiv 0 \pmod{p-1}$. Hence, $n > rp$. Consider the invariance of f under ω . We have $\omega x^n = x^n + nx^{n-1}y + \dots$ and if $r > 1$, then 4.1(6) shows that the term $x^{n-1}y$ cannot cancel with any other term. This implies that $n \equiv 0 \pmod{p}$ which is not possible because $n \equiv 0 \pmod{p-1}$ and $n < p^2 - p$.

Hence, from now on we only need to investigate the case of $r = 1$. Assume there is an invariant of the form

$$f = \sum_{i=0}^{p-1} \lambda_i x^i y^{n-i} + x^n, \text{ for } p \leq n < p^2 - p.$$

By sparseness, we know that $n \equiv 0 \pmod{p-1}$ and $\lambda_i = 0$ except whenever $2i \equiv 0 \pmod{p-1}$. Hence,

$$f = \lambda_0 y^n + \lambda_1 x^{\frac{p-1}{2}} y^{n-\frac{p-1}{2}} + \lambda_2 x^{p-1} y^{n-p+1} + x^n.$$

Let us investigate the action of ω on x^n . Let $n = k(p-1)$ for some $k = 2, \dots, p-1$. In the following computation we use proposition 4.1(5) and lemma 5.1:

$$\begin{aligned}
\omega x^n &= y^n + x^n + \sum_{i=1}^{p-1} \binom{n}{i} x^i y^* + \sum_{s=1}^{p-1} \sum_{\substack{i=p \\ i \equiv s \pmod{p-1}}}^{n-1} \binom{n}{i} x^s y^* \\
&= y^n + x^n + \sum_{i=1}^{p-1} \binom{n}{i} x^i y^* + \sum_{s=1}^{p-2} \sum_{\substack{i=p \\ i \equiv s \pmod{p-1}}}^{n-1} \binom{n}{i} x^s y^* + \sum_{\substack{i=p \\ i \equiv 0 \pmod{p-1}}}^{n-1} \binom{n}{i} x^{p-1} y^* \\
&= y^n + x^n + \sum_{i=1}^{p-1} \binom{n}{i} x^i y^* + \sum_{s=1}^{p-2} \sum_{t=1}^{k-1} \binom{n}{s+t(p-1)} x^s y^* + \sum_{t=1}^{k-2} \binom{n}{(t+1)(p-1)} x^{p-1} y^* \\
&= y^n + x^n + \sum_{i=1}^{p-2} \sum_{t=0}^{k-1} \binom{n}{i+t(p-1)} x^i y^{n-i} \\
&= y^n + x^n + \sum_{i=1}^{p-2} (-1)^i x^i y^{n-i}
\end{aligned}$$

Thus, if $\omega f = f$ we can compare the coefficients of y^n and xy^{n-1} in f and ωf to get $\lambda_1 = 0$, $\lambda_2 = -1$ and so $f = \lambda_0 y^n - x^{p-1} y^{n-p+1} + x^n$. If we compute the action of $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ on f we see that if f is invariant then $\lambda_0 = 1$. The conclusion is that the invariants of positive degree in A for $r = 1$ are contained in the \mathbb{F}_p -span of the polynomials γ_i for $i = 2, \dots, p-1$.

To finish the proof we have to prove that the polynomials γ_i are invariant elements in the coinvariant algebra A . This follows immediately from the computation of ωf above and the (easier) computation of the action of $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ on each γ_i . \square

This last theorem settles the computation of the ideal of stable invariants of the groups L^r for $r > 1$. Since the ring of coinvariants of these groups has no invariants of positive degree, the ideal of stable invariants coincides with the ideal of ordinary invariants.

When $r = 1$ the situation is very different. To compute the stable invariants we need to investigate the quotient Q of the ring of coinvariants P_{L^1} by the ideal of its invariants of positive degree, as computed in theorem 5.2.

Proposition 5.3. *Let $Q := P/\langle d_1, \delta, \mu, \gamma_2, \dots, \gamma_{p-1} \rangle$. Then*

- (1) $Q = P/\langle d_1, \delta, \gamma_2, x^{p-1} y^{2p-2} \rangle$.
- (2) Q has an \mathbb{F}_p -basis as follows

$$\Theta = \left\{ x^i y^j \mid \begin{array}{l} 0 \leq i \leq p-1, 0 \leq j \leq 2p-2 \\ i+j \neq 3p-3 \end{array} \right\} \cup \{x^i \mid p \leq i \leq 2p-3\}.$$

- (3) Q has no L^1 -invariants of positive degree.

Proof. To see that Θ generates Q , we will show that the monomials in $\Omega^1 - \Theta$ vanish or become redundant in Q . Notice that $\gamma_2 = x^{2(p-1)} + y^{2(p-1)} - x^{p-1} y^{p-1}$ hence $x^{2(p-1)} = x^{p-1} y^{p-1} - y^{2(p-1)}$ in Q . On the other hand, $x\gamma_2 = x^{2p-1} + \langle d_1, \delta \rangle$ by 4.1(5) and so $x^{2p-1} = 0$ in Q . By the same argument, $y^{2p-1} = 0$ in Q . Finally, $\gamma_3 = x^{3(p-1)} - x^{p-1} y^{2(p-1)} + y^{3(p-1)}$ hence $x^{p-1} y^{2(p-1)} = 0$ in Q and we have seen that Θ generates Q and this also shows part (1) of the proposition.

Let us see now that the elements in Θ are linearly independent in Q . Since $\Theta \subset \Omega^1$ and Ω^1 is a basis of $P/\langle d_1, \delta \rangle$, it is enough to show that a linear combination

$$f = \sum_{i=n-2p+2}^{p-1} \lambda_i x^i y^{n-i}$$

in degree n with $2p-1 \leq n < 3p-3$ such that $f + g\gamma_2 \in \langle d_1, \delta \rangle$ for some g of positive degree must have all coefficients $\lambda_i = 0$, $n-2p+2 \leq i \leq p-1$. Let $g = \sum_{i=0}^k \mu_i x^i y^{k-i}$ for $k = n-2p+2$, $1 \leq k \leq p-2$. From 4.1(5), we get the following identities modulo $\langle d_1, \delta \rangle$:

$$\begin{aligned} f + g\gamma_2 &= f + \sum_{i=0}^k \mu_i x^{i+2p-2} y^* - \sum_{i=0}^k \mu_i x^{i+p-1} y^* + \sum_{i=0}^k \mu_i x^i y^* \\ &= f + \mu_k x^n + \sum_{i=0}^{k-1} \mu_i x^{i+2p-2} y^* - \mu_0 x^{p-1} y^* - \sum_{i=1}^k \mu_i x^{i+p-1} y^* + \sum_{i=0}^k \mu_i x^i y^* \\ &= f + \mu_k x^n + \sum_{i=0}^{k-1} \mu_i x^i y^{n-i} \\ &= \sum_{i=k}^{p-1} \lambda_i x^i y^{n-i} + \mu_k x^{k+2p-2} + \sum_{i=0}^{k-1} \mu_i x^i y^{n-i}. \end{aligned}$$

All monomials in the last term above are in Ω^1 and so they are linearly independent modulo $\langle c_0, \delta \rangle$. Hence, $f + g\gamma_2 \in \langle d_1, \delta \rangle$ implies $\lambda_i = 0$ for $k \leq i \leq p-1$.

Notice that if $p = 3$ we have $x^{p-1} y^{2p-2} \in \langle d_1, \delta, \gamma_2 \rangle$ and so

$$Q = P/\langle d_1, \delta, \gamma_2 \rangle \text{ for } p = 3.$$

To prove that there are no L^1 -invariants of positive degree in Q we proceed in a similar way as in the proof of 5.2. Suppose there is an invariant $f = \sum_{i=k}^{p-1} \lambda_i x^i y^{n-i}$ in degree n for $2p-2 < n < 3p-3$. Then

$$\omega f = \sum_{i=k}^{p-1} \sum_{s=0}^i \binom{i}{s} \lambda_i x^s y^{n-s} \equiv \sum_{s=k}^{p-1} \left(\sum_{i=s}^{p-1} \binom{i}{s} \lambda_i \right) x^s y^{n-s}.$$

Then, as in the proof of 5.2, $\omega f = f$ in Q implies $\lambda_i = 0$ for $k+1 \leq i \leq p-1$ and f is a scalar multiple of the monomial $x^k y^{2p-2}$ which is not invariant under $D(\zeta, \zeta^{-1})$. \square

The computation of the stable invariants of the groups L^r is done:

Theorem 5.4. *The sequence of ideals of stable invariants of the reflection groups L^r is as follows:*

- (1) If $r > 1$ then $J_\infty(L^r) = J_1(L^r) = \langle d_1, \delta^r \rangle$.
- (2) $J_\infty(L^1) = J_2(L^1) = \langle d_1, \delta, \gamma_2, x^{p-1} y^{2p-2} \rangle \supsetneq J_1(L^1) = \langle d_1, \delta \rangle$. \square

Let us consider now the decomposable groups $U_{r,s}$ for $r, s|p-1$. In proposition 3.2 we have computed the ideal of ordinary invariants of these groups

$$J_1(U_{r,s}) = \langle x^r, (y^p - x^{p-1} y)^s \rangle = \langle x^r, y^{sp} \rangle.$$

Theorem 5.5. *The sequence of ideals of stable invariants of the reflection groups $U_{r,s}$ is as follows:*

- (1) If $r > 1$ then $J_\infty(U_{r,s}) = J_1(U_{r,s}) = \langle x^r, y^{sp} \rangle$.
- (2) $J_\infty(U_{1,s}) = J_2(U_{1,s}) = \langle x, y^s \rangle \supsetneq J_1(U_{1,s}) = \langle x, y^{sp} \rangle$.

Proof. It is obvious that the ring of coinvariants has a monomial basis consisting of the divisors of $x^{r-1}y^{sp-1}$. Invariance under the matrices $D(\zeta^{(p-1)/r}, 1)$ and $D(1, \zeta^{(p-1)/s})$ implies that an invariant of positive degree must be a multiple of y^{si} for $i = 1, \dots, p-1$. If $r > 1$ none of these monomials is invariant under ω' while all of them are invariant if $r = 1$. This computes $J_2(U_{r,s})$ and the theorem follows. \square

Some particular cases of this theorem were considered in [16].

6. IDEALS OF GENERALIZED INVARIANTS

In this section we compute the ideal of generalized invariants for any set of reflections $\mathcal{S} \subset GL_2(\mathbb{F}_p)$. The computation of the ideal of generalized invariants is trivial in those cases in which the stable invariants of the group $G(\mathcal{S})$ coincide with the ordinary invariants of $G(\mathcal{S})$ and this happens, in particular, if the order of $G(\mathcal{S})$ is prime to p . Hence, theorems 3.1, 5.4 and 5.5 imply that in the case of rank two the computation of the generalized invariants is only relevant for those sets of reflections \mathcal{S} which generate one of the groups $L^1, U_{1,s}$ for $s|p-1$.

Theorem 6.1. *Let \mathcal{S} be a set of reflections generating $U_{r,s}$ for some $r, s|p-1$. Then*

$$I(\mathcal{S}) = \begin{cases} \langle x^r, y^{sp} \rangle & \text{if } r > 1 \text{ or } \mathcal{S} \text{ contains an element of order } p; \\ \langle x, y^s \rangle & \text{otherwise.} \end{cases}$$

Proof. We can assume $r = 1$. We have

$$\langle x, y^{sp} \rangle = J_1(U_{1,s}) \subseteq I(\mathcal{S}) \subseteq J_\infty(U_{1,s}) = \langle x, y^s \rangle.$$

Hence, $I(\mathcal{S}) = \langle x, y^k \rangle$ for some k with $s \leq k \leq sp$. This value of k is characterized by the fact that

$$\Delta_\alpha(y^k) \in \langle x \rangle \text{ for any } \alpha \in \mathcal{S}.$$

It is not difficult to compute the values of $\Delta_\alpha(y^k)$ modulo x for any reflection $\alpha \in U_{1,s}$:

$$\Delta_\alpha(y^k) = \begin{cases} \lambda k y^{k-1} + \langle x \rangle & \text{for } \alpha = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, \lambda \neq 0 \\ \frac{\beta^k - 1}{\beta - 1} y^{k-1} + \langle x \rangle & \text{for } \alpha = \begin{pmatrix} 1 & \lambda \\ 0 & \beta \end{pmatrix}, \beta \neq 0, 1 \end{cases}$$

If $s = 1$ then we are dealing with the cyclic group of order p and \mathcal{S} contains only powers of ω' . In this case it is easy to conclude that $I(\mathcal{S}) = \langle x, y^p \rangle$. Assume $s > 1$ and let

$$\mathcal{S} = \left\{ \begin{pmatrix} 1 & \lambda_i \\ 0 & \beta_i \end{pmatrix}, i = 1, \dots, n \right\}.$$

We have that s is the l.c.m. of the orders of all β_i and so $s|k$ by the computation above. If \mathcal{S} also contains a reflection of order p then $p|k$ and $k = ps$. The theorem follows. \square

In the case of the groups L^r we obtain that the generalized invariants coincide with the ordinary invariants.

Theorem 6.2. *Let \mathcal{S} be a set of reflections generating L^r . Then $I(\mathcal{S}) = J_1(L^r) = \langle d_1, \delta^r \rangle$.*

Proof. As said before, we just need to consider the case of L^1 . We know that

$$\langle \delta, d_1 \rangle = J_1(L^1) \subseteq I(\mathcal{S}) \subseteq J_\infty(L^1) = \langle \delta, \gamma_2, x^{p-1}y^{2p-2}, d_1 \rangle.$$

We also know that $I(\mathcal{S})$ is generated by a regular sequence of two polynomials, hence for each generating set of reflections \mathcal{S} we can find a polynomial $f(\mathcal{S})$ such that

$$I(\mathcal{S}) = \langle \delta, f(\mathcal{S}) \rangle.$$

It is clear that $|f(\mathcal{S})| \leq |d_1| = p(p-1)$ and the theorem is proven if we show that $|f(\mathcal{S})| = p(p-1)$. On the other hand, $f(\mathcal{S}) \in \langle \delta, \gamma_2, x^{p-1}y^{2p-2}, d_1 \rangle - \langle \delta \rangle$ hence $|f(\mathcal{S})| \geq 2p-2$. Also, $f(\mathcal{S})$ has the property that

$$\Delta_\alpha(f(\mathcal{S})) \in \langle \delta \rangle \text{ for any } \alpha \in \mathcal{S}.$$

Let f be any polynomial of degree n with $2(p-1) \leq n < p^2 - p$. Using the base Ω^1 we can write

$$f = \lambda_n x^n + \sum_{i=0}^{p-1} \lambda_i x^i y^{n-i} + \langle \delta \rangle.$$

Let us investigate the action of the operator Δ associated to the reflection ω on f modulo $\langle \delta \rangle$. We have

$$\begin{aligned} \Delta(f) &= \lambda_n \sum_{j=0}^{n-1} \binom{n}{j} x^j y^* + \sum_{i=1}^{p-1} \lambda_i \sum_{j=0}^{i-1} \binom{i}{j} x^j y^* + \langle \delta \rangle \\ &= \lambda_n \sum_{j=0}^{n-1} \binom{n}{j} x^j y^* + \sum_{j=0}^{p-2} \sum_{i=j+1}^{p-1} \binom{i}{j} \lambda_i x^j y^* + \langle \delta \rangle \end{aligned}$$

Checking the coefficient of x^{n-1} in the formulas above we get that if $\Delta(f) \in \langle \delta \rangle$ then $n\lambda_n = 0$.

Let us first consider the case in which $\lambda_n = 0$. Then, $\Delta(f) \in \langle \delta \rangle$ yields a system of linear equations

$$\sum_{i=j+1}^{p-1} \binom{i}{j} \lambda_i = 0, \quad j = 0, \dots, p-2$$

which has only the trivial solution $\lambda_i = 0, i = 1, \dots, p-1$. Hence, $f = \lambda_0 y^n$.

If $\lambda_n \neq 0$ then $n = mp$ with $2 \leq m < p-1$. Notice that

$$\begin{aligned} \Delta(x^{mp}) &= \frac{(x^p + y^p)^m - x^{mp}}{y} = \sum_{i=0}^{m-1} \binom{m}{i} x^{ip} y^* \\ &= y^{mp-1} + \sum_{i=1}^{m-1} \binom{m}{i} x^{ip} y^* = y^{mp-1} + \sum_{i=1}^{m-1} \binom{m}{i} x^i y^* + \langle \delta \rangle. \end{aligned}$$

Hence, taking $\lambda_n = 1$ we have

$$\Delta(f) = \sum_{i=0}^{m-1} \binom{m}{i} x^i y^* + \sum_{i=0}^{p-2} \left(\sum_{j=i+1}^{p-1} \binom{j}{i} \lambda_j \right) x^i y^* + \langle \delta \rangle$$

and $\Delta(f) \in \langle \delta \rangle$ yields a system of linear equations like before

$$\sum_{i=j+1}^{p-1} \binom{i}{j} \lambda_i = \begin{cases} -\binom{m}{j} & j = 0, \dots, m-1 \\ 0 & j = m, \dots, p-2. \end{cases}$$

It is not difficult to find the unique solution of these equations which is $\lambda_m = -1$, $\lambda_i = 0$, $0 < i \neq m$.

The conclusion so far is that the only polynomials modulo $\langle \delta \rangle$ in degree n with $2(p-1) \leq n < p^2 - p$ such that $\Delta(f) \in \langle \delta \rangle$ are the scalar multiples of y^n and

$$h_m := x^{mp} + \lambda y^{mp} - x^m y^{m(p-1)}$$

for $2 \leq m < p-1$ and any λ .

Recall that $\overline{\Delta}$ is the operator associated to the reflection ω' . Checking the coefficient of x^{n-1} , it is clear that $\overline{\Delta}(y^n) \notin \langle \delta \rangle$. Let us investigate if $\overline{\Delta}(h_m) \in \langle \delta \rangle$ for some value of m . We have

$$\begin{aligned} \overline{\Delta}(h_m) &= \lambda x^{mp-1} + \lambda m x^{p-1} y^* + \lambda \sum_{j=1}^{m-2} \binom{m}{j+1} x^j y^* \\ &\quad - \sum_{r=0}^{m(p-1)-1} \binom{m(p-1)}{r+1} x^{m+r} y^* + \langle \delta \rangle. \end{aligned}$$

If we use 4.1(5) to write $\overline{\Delta}(h_m)$ in the basis Ω^1 we see that the coefficient of $x^m y^*$ is equal to

$$\sum_{j=0}^{m-1} \binom{m(p-1)}{1+j(p-1)} \equiv -1 \pmod{p}$$

(by lemma 5.1) hence $\overline{\Delta}(h_m) \notin \langle \delta \rangle$.

All the arguments so far prove that if \mathcal{S} contains the reflections ω and ω' , then we can choose $f(\mathcal{S}) = d_1$ and the theorem is proven in this case. The general case follows easily. Since \mathcal{S} generates $L^1 = SL_2(\mathbb{F}_p)$, up to a conjugation in $GL_2(\mathbb{F}_p)$ we can assume that \mathcal{S} contains ω and some other reflection $\alpha = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$. Notice that ω' is equal to some power of α . Then, lemma 2.4 in [16] gives

$$I(\mathcal{S}) = I(\mathcal{S} \cup \{\omega'\}) = \langle \delta, d_1 \rangle.$$

□

In these results we find examples of the following two phenomena (already noted in [12] and [16]):

- (1) The ideal of generalized invariants $I(\mathcal{S})$ depends on the set of reflections \mathcal{S} , not just on the reflection group $G(\mathcal{S})$ they generate.
- (2) The ideal of generalized invariants $I(\mathcal{S})$ can be strictly smaller than the ideal of stable invariants $J_\infty(G(\mathcal{S}))$.

In particular, γ_2 is a stable invariant for L^1 but it is not a generalized invariant for any set of generating reflections of L^1 . We finish this section providing an explicit sequence of length $2p-2$ of Δ -operators which does not vanish on γ_2 . The following result contains also some computations of these operators which may be useful elsewhere.

Proposition 6.3. *Let Δ and $\overline{\Delta}$ be as before. Then*

- (1) *The following recurrence formula holds for $i \geq 1$, $j \geq 0$:*

$$\Delta^i(x^{i+j}) = \sum_{k=0}^j \binom{i+j}{i+k-1} (\Delta^{i-1}(x^{i+k-1})) y^*$$

- (2) $\Delta^i(x^i) = i!$ for $i \geq 0$.

- (3) $\Delta^i(x^{i+1}) = (i+1)!(x + iy/2)$ for $i \geq 0$.
- (4) $\Delta^i(x^p z) = iy^{p-1}\Delta^{i-1}(z) + iy^p\Delta^i(z) + x^p\Delta^i(z)$ for $i \geq 0$ and any $z \in P$.
- (5) $\Delta^{p-2}(x^{2p-2}) = (p-2)!(x^p + y^p - 2xy^{p-1})$.
- (6) $\Delta^{p-2}(\gamma_2) = (p-2)!(x^p - xy^{p-1})$.
- (7) $\Delta\bar{\Delta}^{p-1}\Delta^{p-2}(\gamma_2) \neq 0$. Hence, γ_2 is not a generalized invariant for the reflections ω and ω' .

Proof. The proof of each of these formulas is easy and can be left as an exercise. To prove (1), decompose $\Delta^i = \Delta^{i-1}\Delta$. (2) and (3) follow immediately from (1) for $j = 0$ and $j = 1$, respectively, plus induction. (4) is proven by induction on i . To prove (5), write $\Delta^{p-2}x^{2p-2} = \Delta^{p-2}(x^p x^{p-2})$ and use (3) and (4). (6) follows from (5) and (3). (7) is then obvious from (6) and (2). \square

7. MODULAR RANK TWO REFLECTION GROUPS IN TOPOLOGY

Real reflection groups appear in topology as Weyl groups of compact Lie groups and reflection groups over \mathbb{F}_p appear as mod p reductions of these Weyl groups. Then, the invariant theory of these groups is crucial in understanding the cohomology of the compact Lie groups and the cohomology of their classifying spaces. Actually, the theory of generalized invariants was invented (see [9] and [11]) in order to understand the mod p cohomology of the compact connected Lie groups. Furthermore, the family of compact Lie groups has been extended in several directions (Kac-Moody groups [15], p -compact groups [10], p -local finite groups [7]) and in each case, the invariant theory of reflection groups over \mathbb{F}_p plays an important role in understanding the properties of these objects, mainly its cohomology.

Let K be a compact connected Lie group or, more in general, a compact form of a Kac-Moody group (in the sense of [15]), with maximal torus T . Let M be the weight lattice and let $\mathcal{S} = \{s_1, \dots, s_n\}$ be the reflections with respect to a set of simple roots. \mathcal{S} generates the Weyl group W of K and the symmetric algebra $S(M)$ can be identified to the cohomology of the classifying space BT . Choose a prime p and denote M_p the mod p reduction of M and $W_p \subset GL_n(\mathbb{F}_p)$ the mod p reduction of the Weyl group W , acting on M_p . There is a map

$$\psi : S(M_p) = H^*(BT; \mathbb{F}_p) \longrightarrow H^*(K/T; \mathbb{F}_p).$$

Then, the kernel of this map coincides with the ideal of generalized invariants $I(\mathcal{S})$:

$$\text{Ker } \psi = I(\mathcal{S}).$$

This fundamental result is due to Kac ([11], see also [17] and Theorem 6.1 in [15]).

Hence, some of the groups that we have investigated in the preceding sections should appear as mod p reductions of Weyl groups. If the rank is two, then the Weyl group is either cyclic of order two or dihedral. It is easy to check that among the groups that we have considered in this paper (i.e. reflection groups in $GL_2(\mathbb{F}_p)$ of order divisible by p), the only dihedral groups are $GL_2(F_2)$ for $p = 2$, and $U_{1,2}$, $U_{2,1}$, $U_{2,2}$ for any prime. Hence, these and the cyclic group $U_{1,1}$ for $p = 2$, are the only groups of order divisible by p that may appear as mod p reductions of Weyl groups.

It is not difficult to compute W_p for all compact connected Lie groups of rank two. We get groups of order divisible by p in the following cases:

- $SU(3)$ gives $W_2 = GL_2(F_2)$ and $W_3 = U_{2,1}$ with $\mathcal{S} = \left\{ \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$.
- $Sp(2)$ gives $W_2 = U_{1,1}$.

- G_2 gives $W_2 = GL_2(F_2)$ and $W_3 = U_{2,2}$ with $\mathcal{S} = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$.
- $PSp(2)$ gives $W_2 = GL_2(F_2)$.
- $PSU(3)$ gives $W_2 = GL_2(F_2)$ and $W_3 = U_{1,2}$ with $\mathcal{S} = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$.
The case of this group at the prime 3 is the only case in which there is a discrepancy between ordinary and generalized invariants. We have $J_1 = \langle x, y^6 \rangle$ while $I(\mathcal{S}) = \langle x, y^2 \rangle$.
- $U(2)$ gives $W_2 = U_{1,1}$.

We obtain all possible reflection groups, but only for very small primes. If we extend our scope to rank two Kac-Moody groups, then these reflection groups appear as mod p Weyl groups W_p for all primes. For any pair of positive integers a, b with $ab > 4$, let us denote $K(a, b)$ the compact form of the simply connected Kac-Moody group associated to the Cartan Matrix $\begin{pmatrix} 2 & -a \\ -b & 2 \end{pmatrix}$. The groups $K(a, b)$, their Weyl groups, and the cohomology of the classifying spaces $BK(a, b)$ were investigated in [3]. From Propositions 7.1, 6.2 and 3.2 in [3] one deduces the following:

- $K(a, b)$ gives $W_p = U_{2,2}$ for any prime $p > 2$ which divides a but not b .
- $K(a, b)$ gives $W_p = U_{2,1}$ for any prime $p > 2$ which divides $4 - ab$.
- $PK(a, b)$ gives $W_p = U_{1,2}$ for any prime $p > 2$ such that $p \nmid 4 - ab$ and $p^2 \nmid 4 - ab$.

The identifications of these Weyl groups and their invariant theory was crucial in the cohomological computations in [3].

The rank two reflection groups which are not dihedral groups (i.e. the groups L^r and $U_{a,b}$ for $a > 2$ or $b > 2$) could appear as mod p reductions W_p of Weyl groups of p -compact groups. The classification of all p -compact groups is available (see [4] and [5]) and if we check all the cases of rank two we see that there is only one p -compact group which realizes a modular rank two reflection group not considered above. The relevant prime is $p = 3$ and the reflection group is $GL_2(\mathbb{F}_3)$. It turns out that this reflection group is the group number 12 in the list of complex reflection groups ([18]) and it can be lifted to a 3-adic reflection group W . In 1984 Zabrodsky proved the existence of a 3-compact group of rank two X_{12} having W as Weyl group ([22], see also [1]). This completes the list of reflection groups in $GL_2(\mathbb{F}_p)$ of order divisible by p that have appeared (so far) as mod p Weyl groups of compact Lie groups or other topological groups generalizing compact Lie groups.

REFERENCES

- [1] J. Aguadé, *Constructing modular classifying spaces*. Israel J. Math. 66, nos 1–3 (1989), 23–40.
- [2] J. Aguadé, A. Ruiz, *Cohomology of Kac-Moody groups over a finite field*. Algebr. Geom. Topol. 13 (2013), no. 4, 2207–2238.
- [3] J. Aguadé, C. Broto, N. Kitchloo, L. Saumell, *Cohomology of classifying spaces of central quotients of rank two Kac-Moody groups*. J. Math. Kyoto Univ. 45 (2005), no. 3, 449–488.
- [4] K. K. S. Andersen, J. Grodal, J. M. Møller, A. Viruel, *The classification of p -compact groups for p odd*. Ann. of Math. (2) 167 (2008), no. 1, 95–210.
- [5] K. K. S. Andersen, J. Grodal, *The classification of 2-compact groups*. J. Amer. Math. Soc. 22 (2009), no. 2, 387–436.
- [6] D. J. Benson, *Polynomial Invariants of Finite Groups*, LMS Lecture Notes Series, vol. 190, Cambridge Univ. Press, Cambridge, 1993.
- [7] C. Broto, R. Levi, B. Oliver, *The homotopy theory of fusion systems*. J. Amer. Math. Soc. 16 (2003), no. 4, 779–856.
- [8] H. E. A. Campbell, I. P. Hughes, R. J. Shank, D. L. Wehlau, *Bases for rings of coinvariants*, Trans. Groups 1, No. 4 (1996), 307–336.

- [9] M. Demazure, *Invariants symétriques entiers des groupes de Weyl et torsion*. Invent. Math. 21 (1973), 287–301.
- [10] W. G. Dwyer, C. W. Wilkerson, *Homotopy fixed-point methods for Lie groups and finite loop spaces*. Ann. of Math. (2) 139 (1994), no. 2, 395–442.
- [11] V. G. Kac, *Torsion in cohomology of compact Lie groups and Chow rings of reductive algebraic groups*. Invent. Math. 80 (1985), no. 1, 69–79.
- [12] V. G. Kac, D. H. Peterson, *Generalized invariants of groups generated by reflections*. Geometry today (Rome, 1984), 231–249, Progr. Math., 60, Birkhäuser Boston, Boston, MA, 1985.
- [13] G. Kemper, *Calculating invariant rings of finite groups over arbitrary fields*, J. Symb. Comp. 21 (1996), 351–366.
- [14] G. Kemper, G. Malle, *The finite irreducible linear groups with polynomial ring of invariants*. Transform. Groups 2 (1997), no. 1, 57–89.
- [15] N. Kitchloo, *On the Topology of Kac-Moody groups*. Math. Z. 276 (2014), 727–756.
- [16] F. Neumann, M. D. Neusel, L. Smith, *Rings of generalized and stable invariants of pseudoreflections and pseudoreflection groups*. J. Alg. 182 (1996) 85–122.
- [17] F. Neumann, M. D. Neusel, L. Smith, *Rings of generalized and stable invariants and classifying spaces of compact Lie groups*. Higher homotopy structures in topology and mathematical physics (Poughkeepsie, NY, 1996), 267–285, Contemp. Math., 227, Amer. Math. Soc., Providence, RI, 1999.
- [18] G. C. Shephard, J. A. Todd, *Finite unitary reflection groups*, Canadian J. Math. 6 (1954), 274–304.
- [19] L. Smith, *Polynomial Invariants of Finite Groups*. A K Peters, Wellesley, Mass., 1995.
- [20] N. E. Steenrod, *Cohomology operations*. Lectures by N. E. Steenrod written and revised by D. B. A. Epstein. Annals of Mathematics Studies, No. 50 Princeton University Press, Princeton, N. J. 1962.
- [21] M. Suzuki, *Group theory. I*. Grundlehren der Mathematischen Wissenschaften, 247. Springer-Verlag, Berlin-New York, 1982.
- [22] A. Zabrodsky, *On the realization of invariant subgroups of π_*X* . Trans. Amer. Math. Soc. 285 (1984), 467–496.

E-mail address: Jaume.Aguade@uab.cat

DEPARTAMENT DE MATEMÀTIQUES, UNIVERSITAT AUTÒNOMA DE BARCELONA, 08193 Cerdanyola del Vallès, Spain.